(54) SOFTWARE STORAGE MEDIUM, SOFTWARE READER, AND SOFTWARE MANAGEMENT SYSTEM

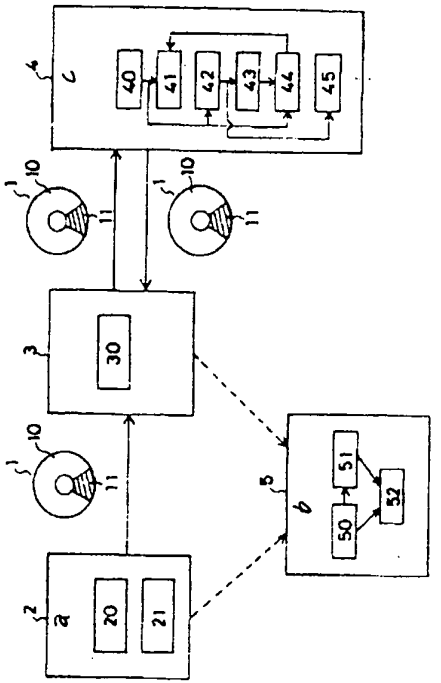
(11) 5-298085 (A) (43) 12.11.1993 (19) JP
(21) Appl. No. 4-105034 (22) 24.4.1992

(71) FUJITSU LTD (72) RYOTA AKIYAMA(2)

(51) **Int. Cl⁵. G06F9/06,G06F12/14**

PURPOSE: To provide a storage medium which promotes prevention of the wrong use of software circulated to distribution routes, a reader for software in this storage medium, and a management system which checks the wrong use of software in the storage medium.

CONSTITUTION: A hybrid storage medium consisting of an un-rewritable storage area 10 and a rewritable storage area 11 is prepared as the storage medium, and password information of software to be presented is recorded in the unrewritable storage area 10, and password information consisting of key information for deciphering of ciphered software and the permitted frequency in use of software is recorded in the rewritable storage area 11. Meanwhile, the reader reduces the permitted frequency use of the storage medium in accordance with the use of software to inhibit software from being used more than the permitted frequency in use, and the management system checks the wrong use of software in accordance with the display value of the permitted frequency in use of the storage medium.



2: shipping source, 3: relaying destination, 4: user side, 5: management center, a: shipping source device, b: relaying destination device, c: software data reader, d: management device

[3]-#1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－298085

(43)公開日　平成５年(1993)11月12日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	9/06	４５０	Ｌ　7232－5Ｂ		
	12/14	３２０	Ｆ　9293－5Ｂ		

審査請求　未請求　請求項の数７(全 10 頁)

(21)出願番号　特願平4－105034

(22)出願日　平成４年(1992)４月24日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　森田　寛　(外１名)

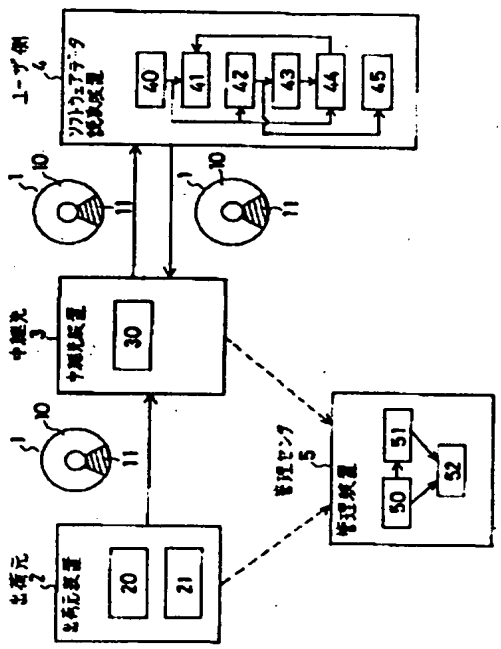
(54)【発明の名称】　ソフトウェア記憶媒体、ソフトウェア読取装置及びソフトウェア管理システム

(57)【要約】

【目的】本発明は、流通経路を流布するソフトウェアの不正使用の防止を促進できる記憶媒体と、その記憶媒体のソフトウェアの読取装置と、その記憶媒体のソフトウェアの不正使用をチェックする管理システムに関する。

【構成】記憶媒体として、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体を用意し、この書換不可能記憶領域１０に、提供対象のソフトウェアの暗号情報を記録するとともに、この書換可能記憶領域１１に、暗号ソフトウェア復号用の鍵情報とソフトウェアの使用可能回数との暗号情報を記録する構成を採り、一方、読取装置は、ソフトウェア使用に応じて記憶媒体の使用可能回数を減じていくとともに、使用可能回数以上のソフトウェア使用を禁止していく構成を取り、一方、管理システムは、記憶媒体の使用可能回数の表示値に従って、ソフトウェアの不正使用をチェックしていくように構成する。

本発明の原理構成図



1

【特許請求の範囲】

【請求項１】　流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体であって、

ソフトウェア記憶媒体として、書換不可能記憶領域(10)と書換可能記憶領域(11)との混成からなる混成型記憶媒体を用意し、該混成型記憶媒体の書換不可能記憶領域(10)に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、該混成型記憶媒体の書換可能記憶領域(11)に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採ることを、

特徴とするソフトウェア記憶媒体。

【請求項２】　請求項１記載のソフトウェア記憶媒体において、

ソフトウェアの使用可能回数の初期値が、流通経路途中で記録されるよう構成されることを、

特徴とするソフトウェア記憶媒体

【請求項３】　請求項１又は２記載のソフトウェア記憶媒体において、

暗号ソフトウェア保護情報を多重構成で暗号化していく構成を採るとともに、流通経路途中で、この多重暗号化構成を変更していくよう構成されることを、

特徴とするソフトウェア記憶媒体。

【請求項４】　請求項１、２又は３記載の記録構成を採るソフトウェア記憶媒体に記録される暗号ソフトウェアを読み取るためのソフトウェア読取装置であって、

暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とを復号する第１の復号手段(40)と、

上記第１の復号手段(40)の復号する鍵情報に従って暗号ソフトウェアを復号する第２の復号手段(41)と、

上記第１の復号手段(40)の復号する使用可能回数を使用終了毎に減算することで新たな使用可能回数を算出する算出手段(42)と、

上記算出手段(42)の算出する新たな使用可能回数に従って、ソフトウェア記憶媒体の記録する暗号ソフトウェア保護情報の使用可能回数を更新する更新手段(43)と、

上記第１の復号手段(40)の復号する使用可能回数か、上記算出手段(42)の算出する使用可能回数のいずれか一方がゼロ値を表示するときには、上記第２の復号手段(41)が復号処理を実行できないように制御する抑止手段(44)とを備えることを、

特徴とするソフトウェア読取装置。

【請求項５】　請求項４記載のソフトウェア読取装置において、

使用可能回数の減算値がゼロ値に達するときに新たな使用可能回数となる使用追加回数を設定して、本来の使用可能回数と識別可能となる態様に従いつつ、この新たな使用可能回数に従ってソフトウェア記憶媒体の記録する

2

暗号ソフトウェア保護情報の使用可能回数を更新する設定手段(45)を備えることを、

特徴とするソフトウェア読取装置。

【請求項６】　請求項１、２又は３記載の記録構成を採るソフトウェア記憶媒体に記録されるソフトウェアの使用状態を管理するためのソフトウェア管理システムであって、

流通経路から回収したソフトウェア記憶媒体に記録されるソフトウェアの使用可能回数を集計していくことで、ソフトウェアの使用回数を算出する構成を採るとともに、この使用回数と、流通経路に投入したソフトウェア記憶媒体に記録されるソフトウェアの使用可能回数の集計値とを比較する構成を採って、この比較結果に従ってソフトウェアの不正使用をチェックしていくよう処理することを、

特徴とするソフトウェア管理システム。

【請求項７】　請求項６記載のソフトウェア管理システムにおいて、

ソフトウェアの使用可能回数の集計を、ソフトウェア記憶媒体の識別番号を単位として実行していくよう構成されることを、

特徴とするソフトウェア管理システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関し、特に、流通経路を流布するソフトウェアの不正使用の防止を促進できるソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関する。

【０００２】最近、情報化社会の発達に伴って、コンピュータプログラムや電子出版や娯楽ビデオ等のソフトウェアを、通信ネットワークと連携して、書店等の販売店で販売したり、レンタルビデオ店等のレンタル店で貸し出していくことが行われている。このような流通経路を流布するソフトウェアは、流通段階で、不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されたりというように不正使用にさらされることになる。このような不正使用は、ソフトウェア提供者や販売店やレンタル店の利益を著しく害する。これから、流通経路を流布するソフトウェアの不正使用の防止を実現できる新たな仕組みの構築が叫ばれているのである。

【０００３】

【従来の技術】流通経路を介してソフトウェアを販売し

ていく場合に、販売されるソフトウェアを保護する方法として、従来では、ＩＣプリペードカードを用いる方法を採っていた。

【０００４】すなわち、媒体製造メーカが、ソフトウェアを暗号化してＣＤ－ＲＯＭ等の書き換え不可能な不揮発性の記憶媒体に記録する構成を採って、この暗号ソフトウェアの記憶媒体をソフトウェア市場に提供していくときにあって、ユーザは、この記憶媒体を購入する他に、記憶媒体に記録される暗号ソフトウェアを復号可能とする復号装置と、この復号装置の起動を可能にする使用可能回数の記録されたＩＣプリペードカードとを購入する構成を採る。そして、復号装置は、ＩＣプリペードカードを使って起動されるときに、ＩＣプリペードカードの使用可能回数が残っている場合には、記憶媒体に記録される暗号ソフトウェアの復号を実行し、その使用可能回数を減算していく構成を採る。

【０００５】この構成に従い、ＩＣプリペードカードがなければ記憶媒体を使用することができないことから、ソフトウェアの不正横流しや万引きを防止できるようになるとともに、ＩＣプリペードカードの指定する使用可能回数しか記憶媒体を使用することができないことから、ソフトウェアの不正複写を防止できるようになり、ソフトウェアの不正使用の防止を実現できることになる。なお、ユーザは、使用可能回数の残されていないＩＣプリペードカードについては、発行元の管理センタに郵送することで使用可能回数を再発行してもらったり、通信回線を介して管理センタから新たな使用可能回数を書き込んでもらったりすることになる。

【０００６】

【発明が解決しようとする課題】しかしながら、この従来技術に従うソフトウェアの販売方法では、販売店の側から見ると、ソフトウェアを切り売りしたり、バーゲンセールしたりするといったような販売促進の為のサービスが実行しにくいという問題点がある。また、ユーザの側から見ると、記憶媒体の他に、ＩＣプリペードカードと専用の復号装置とを管理しなければならないという問題点がある。

【０００７】また、安全性から見ると、ＩＣプリペードカードについては、カードコネクタからのデータ盗聴と、カードチップ内の非破壊検査／複製実現とが可能であることから、その安全性が脆弱であるという問題点がある。また、経済性から見ると、高価なＩＣプリペードカードを必要とするとともに、複雑な復号手順を実行する高価な復号装置を必要とするという問題点がある。また、ＩＣプリペードカードの発行元の管理センタ側から見ると、ユーザからの要求が集中することになるという問題点がある。

【０００８】このように、従来技術に従っていると、流通経路を流布するソフトウェアの不正使用を有効に防止することができないことから、ソフトウェア提供者の利益が著しく害されるとともに、販売店の利益が著しく害されることになるという問題点があった。

【０００９】本発明はかかる事情に鑑みてなされたものであって、流通経路を流布するソフトウェアの不正使用の防止を促進できる新たなソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るための新たなソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするための新たなソフトウェア管理システムとの提供を目的とするものである。

【００１０】

【課題を解決するための手段】図１に本発明の原理構成を図示する。この本発明は、特に、流通経路を流布するソフトウェアが販売対象となるときに有効となるものである。

【００１１】１は本発明により構成されるソフトウェア記憶媒体、２はメーカ等の出荷元に設置される出荷元装置、３はレンタル店等の中継先に設置される中継先装置、４はユーザ側に設置されるソフトウェア読取装置、５は管理センタ等に設置される管理装置である。ここで、この管理装置５は、出荷元や中継先に設置されることもある。

【００１２】ソフトウェア記憶媒体１としては、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体が用いられる。出荷元装置２は、ソフトウェア記憶媒体１の書換不可能記憶領域１０に、提供対象のソフトウェアの暗号情報を書き込む第１の書込手段２０と、ソフトウェア記憶媒体１の書換可能記憶領域１１に、提供対象のソフトウェアの保護情報をなす暗号ソフトウェア保護情報を書き込む第２の書込手段２１とを備える。

【００１３】この第２の書込手段２１により書き込まれる暗号ソフトウェア保護情報は、第１の書込手段２０により書き込まれる暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数との暗号情報からなり、先ず最初に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数とが鍵ＫＹでもって暗号化されると、次に、その暗号情報が鍵ＫＳＴでもって暗号化されるというように、多重構成でもって暗号化されていく構成を採ることがある。ここで、使用可能回数については、中継先装置３で書き込まれる構成が採られることもある。

【００１４】中継先装置３は、第２の書込手段２１により書き込まれる暗号ソフトウェア保護情報の暗号構造を変更する暗号構造変更手段３０を備える。この暗号構造変更手段３０は、上述の例で説明するならば、鍵ＫＳＴでもって暗号ソフトウェア保護情報の最終段の暗号構造を復号すると、次に、その復号された暗号情報を鍵ＫＳＴとは異なる鍵ＫＸでもって暗号化するような処理を実行していくことで、暗号ソフトウェア保護情報の暗号構

造を変更する。

【００１５】ソフトウェア読取装置４は、中継先から与えられるソフトウェア記憶媒体１の書換可能記憶領域１１に記録される暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とを復号する第１の復号手段４０と、第１の復号手段４０の復号する鍵情報に従って、ソフトウェア記憶媒体１の書換不可能記憶領域１０に記録される暗号ソフトウェアを復号する第２の復号手段４１と、第１の復号手段４０の復号する使用可能回数を使用終了毎に減算することで新たな使用可能回数を算出する算出手段４２と、算出手段４２の算出する新たな使用可能回数に従って、ソフトウェア記憶媒体１の記録する暗号ソフトウェア保護情報の使用可能回数を更新する更新手段４３と、第１の復号手段４０の復号する使用可能回数か、算出手段４２の算出する使用可能回数のいずれか一方がゼロ値を表示するときには、第２の復号手段４１が復号処理を実行できないように制御する抑止手段４４と、使用可能回数の減算値がゼロ値に達するときに新たな使用可能回数となる使用追加回数を設定して、本来の使用可能回数と識別可能となる態様に従いつつ、この新たな使用可能回数に従ってソフトウェア記憶媒体１の記録する暗号ソフトウェア保護情報の使用可能回数を更新する設定手段４５とを備える。

【００１６】管理装置５は、流通経路に投入されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数を集計する第１の集計手段５０と、流通経路から回収されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数を集計していくことで、ソフトウェアの使用回数を集計する第２の集計手段５１と、第１の集計手段５０の集計値と第２の集計手段５１の集計値とを比較する比較手段５２とを備える。この管理装置５は、ソフトウェアの使用可能回数の集計をソフトウェア記憶媒体１の識別番号を単位として実行していくことがある。

【００１７】

【作用】本発明では、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体１として、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体を用意し、この混成型記憶媒体の書換不可能記憶領域１０に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、書換可能記憶領域１１に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採る。

【００１８】そして、このソフトウェア記憶媒体１のソフトウェアを読み取るユーザ側のソフトウェア読取装置４は、暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能回数を得ると、この使用可能回数がゼロ値を表示していないときには、暗号ソフトウェア保護情報を復号することで得られる暗号ソフトウェア復号用の鍵情報を用いて暗号ソフトウェアを復号するとともに、使用終了毎に使用可能回数を減算して暗号ソフトウェア保護情報を更新し、一方、この使用可能回数がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理する。

【００１９】この構成に従い、本発明では、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになるのである。

【００２０】そして、この構成にあって、中継先は、出荷元の出荷するソフトウェア記憶媒体１の暗号構造を変更してユーザ側に提供し、ユーザ側のソフトウェア読取装置４は、この変更された暗号構造を復号することでソフトウェアの復号を実行していく構成を採ると、出荷元と中継先との間での不正使用は意味をなさないことから、ソフトウェアの不正使用を積極的に防止することができるようになる。

【００２１】更に、本発明では、管理センタ側の管理装置５は、流通経路から回収されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数から、ソフトウェアの使用回数の集計値を算出するとともに、この集計値と、流通経路に投入されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数の集計値とを比較する構成を採って、この比較結果に従ってソフトウェアの不正使用をチェックしていくよう処理する。

【００２２】この構成に従い、本発明では、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。そして、この構成にあって、チェック処理をソフトウェア記憶媒体１の識別番号を単位として実行していく構成を採ると、ソフトウェア記憶媒体１の流通先を記録しておくことで、誰が不正複写等の不正使用をしたのかも特定可能となるのである。

【００２３】

【実施例】以下、実施例に従って本発明を詳細に説明する。図２に、本発明の適用される流通システムの一例を図示する。この図の流通システムは、保護対象のソフトウェアを出荷するメーカと、メーカの出荷するソフトウェアを販売する販売店と、販売店の販売するソフトウェアを購入するユーザと、ソフトウェアの使用状態を管理する管理センタとからなる。

【００２４】このような流通システムに本発明を適用す

る場合、図1で説明した出荷元装置2はメーカに設置され、中継先装置3は販売店に設置され、ソフトウェア読取装置4はユーザ側に設置され、管理装置5は管理センタに設置されることになる。

【0025】図1で説明したように、本発明では、流通経路に置かれるソフトウェアを暗号化して、その暗号情報を混成型記憶媒体の書換不可能記憶領域10に記録するとともに、その暗号ソフトウェアの復号のための鍵情報と、そのソフトウェアの使用可能回数とからなるソフトウェア保護情報を暗号化して、その暗号情報をその混成型記憶媒体の書換可能記憶領域11に記録する構成を採ることで、ソフトウェアの不正使用の防止を実現するものである。

【0026】この混成型のソフトウェア記憶媒体1としては、例えば、書換不可能記憶領域10を光記憶媒体で構成するとともに、書換可能記憶領域11を磁気記憶媒体で構成するような記憶媒体が用いられる。なお、書換不可能記憶領域10を書き換えが不可能であることに対応させて、以下ROM領域と称することがあり、また、書換可能記憶領域11を不揮発性ではあるが、書き換えが可能であることに対応させて、以下RAM領域と称することがある。

【0027】図3に、この記録構成を採る混成型のソフトウェア記憶媒体1に対しての出荷段階での処理を司る出荷元装置2の装置構成の一実施例、図4に、このソフトウェア記憶媒体1に対しての流通段階での処理を司る中継先装置3の装置構成の一実施例、図5に、このソフトウェア記憶媒体1に対しての使用段階での処理を司るソフトウェア読取装置4の装置構成の一実施例、図6に、このソフトウェア記憶媒体1に対しての管理段階での処理を司る管理装置5の装置構成の一実施例を図示する。

【0028】次に、この図3ないし図6に従って、本発明のソフトウェア保護のメカニズムについて詳細に説明する。出荷元装置2は、図3に示すように、第1の暗号化手段200と、第2の暗号化手段201と、第3の暗号化手段202と、第1の鍵管理手段203と、第2の鍵管理手段204と、第3の鍵管理手段205と、使用可能回数設定手段206とを備える。

【0029】この装置構成を採るときにあって、ソフトウェア格納装置から出荷対象の平文のソフトウェアが与えられると、第1の暗号化手段200は、そのソフトウェアを第1の鍵管理手段203の管理する第1の鍵KUでもって暗号化することで、暗号ソフトウェア“E_{KU}（DATA）”を生成して、その暗号ソフトウェアを混成型のソフトウェア記憶媒体1のROM領域にスタンピングする。ここで、同時にスタンピングされる図中の“EOF”は、その暗号ソフトウェアの終了箇所を表示するものである。

【0030】次に、第2の暗号化手段201は、暗号ソフトウェア“E_{KU}（DATA）”の復号に必要となる第1の鍵KUと、使用可能回数設定手段206の設定する使用可能回数Nとを、第2の鍵管理手段204の管理する第2の鍵KYでもって暗号化することで、暗号ソフトウェア保護情報“E_{KY}（KU，N）”を生成する。続いて、第3の暗号化手段202は、第2の暗号化手段201の出力する暗号ソフトウェア保護情報“E_{KY}（KU，N）”を、第3の鍵管理手段205の管理する第3の鍵KSTでもって暗号化することで、暗号ソフトウェア保護情報“E_{KST}（E_{KY}（KU，N））”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体1のRAM領域に電気的に書き込む。

【0031】そして、この図3では省略してあるが、出荷元装置2の図示しない書込手段は、出荷するソフトウェア記憶媒体1の識別番号をそのソフトウェア記憶媒体1のRAM領域に電気的に書き込んでいくよう処理することになる。

【0032】このようにして、出荷元装置2は、混成型のソフトウェア記憶媒体1のROM領域に、提供対象となるソフトウェアの暗号情報を記録し、更に、RAM領域に、その暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とからなるソフトウェア保護情報の暗号情報を記録するとともに、ソフトウェア記憶媒体1の識別番号を記録していくよう処理するのである。

【0033】このような記録構成を採る混成型のソフトウェア記憶媒体1に対しての流通段階での処理を司る中継先装置3は、図4に示すように、復号手段300と、第1の暗号化手段301と、第2の暗号化手段302と、第3の鍵管理手段303と、第4の鍵管理手段304と、変換鍵管理手段305と、入力手段306とを備える。

【0034】この装置構成を採るときにあって、メーカからソフトウェア記憶媒体1を受け取ると、復号手段300は、そのソフトウェア記憶媒体1のRAM領域に書き込まれている暗号ソフトウェア保護情報“E_{KST}（E_{KY}（KU，N））”を、第3の鍵管理手段303の管理する第3の鍵KST（出荷元装置2の第3の鍵管理手段205の管理する鍵と同一のもの）でもって復号することで、暗号ソフトウェア保護情報“E_{KY}（KU，N）”を生成する。

【0035】一方、第2の暗号化手段302は、入力手段306からソフトウェア記憶媒体1の識別番号が入力されてくると、その識別番号を変換鍵管理手段305の管理する変換鍵でもって暗号化することで第4の鍵KXを得て、その第4の鍵KXを第4の鍵管理手段304に登録する。

【C036】復号手段300が復号処理を実行すると、続いて、第1の暗号化手段301は、復号手段300の出力する暗号ソフトウェア保護情報“E_{KY}（KU，

N）”を、第４の鍵管理手段３０４の管理する第４の鍵ＫＸでもって暗号化することで、暗号ソフトウェア保護情報“E_{KX}（E_{KY}（KU，N））”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込む。

【００３７】そして、この図４では省略してあるが、中継先装置３の図示しない書込手段は、販売なのかレンタルなのかを表示する選択コード（この場合は販売である）のような各種の制御情報を、そのソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込んでいくよう処理することになる。

【００３８】このようにして、中継先装置３は、メーカから供給されたソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報“E_{KST}（E_{KY}（KU，N））”を、“E_{KX}（E_{KY}（KU，N））”という別の暗号構造を持つものに書き換えていくよう処理するのである。

【００３９】後述するように、ユーザ側に配置されるソフトウェア読取装置４は、暗号ソフトウェア保護情報“E_{KX}（E_{KY}（KU，N））”を復号する構成を採ることで、ソフトウェア記憶媒体１のＲＯＭ領域に書き込まれている暗号ソフトウェア“E_{KU}（ＤＡＴＡ）”を復号していく構成を採るものである。これから、このように、中継先装置３が、ソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報を、“E_{KST}（E_{KY}（KU，N））”から“E_{KX}（E_{KY}（KU，N））”に書き換えていく構成を採ることで、メーカから販売店の流通経路の間で行われるソフトウェア記憶媒体１の不正使用を完全に排除することが実現できることになる。

【００４０】このような記録構成を採る混成型のソフトウェア記憶媒体１のソフトウェアを読み取るソフトウェア読取装置４は、図５に示すように、第１の暗号化手段４００と、第２の暗号化手段４０１と、第３の暗号化手段４０２と、第４の暗号化手段４０３と、第１の復号手段４０４と、第２の復号手段４０５と、第３の復号手段４０６と、状態表示メモリ４０７と、カウンタ４０８と、比較手段４０９と、書込手段４１０と、出力手段４１１とを備える。

【００４１】この装置構成を採るときにあって、ユーザが販売店から購入したソフトウェア記憶媒体１の読み取りを指示すると、先ず最初に、第１の暗号化手段４００は、そのソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている識別番号を、規定の変換鍵でもって暗号化することで、中継先装置３の第４の鍵管理手段３０４の管理する鍵と同一の鍵ＫＸを生成する。次に、第１の復号手段４０４は、ソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報“E_{KX}（E_{KY}（KU，N））”を、この第１の暗号化手段４００の生成した鍵ＫＸでもって復号することで、暗号ソフトウェア保護情報“E_{KY}（KU，N）”を生成する。

【００４２】続いて、第２の復号手段４０５は、バッテリバックアップされた状態表示メモリ４０７に格納されている鍵ＫＹ（出荷元装置２の第２の鍵管理手段２０４の管理する鍵と同一のもの）を読み出し、第１の復号手段４０４の出力する暗号ソフトウェア保護情報“E_{KY}（KU，N）”を、この鍵ＫＹでもって復号することで、ソフトウェア記憶媒体１に記録されている暗号ソフトウェア“E_{KU}（ＤＡＴＡ）”の復号に必要となる鍵ＫＵと、そのソフトウェアの使用可能回数Ｎ（購入当初は、出荷元装置２の使用可能回数設定手段２０６の設定する値と一致）とを生成する。そして、第２の復号手段４０５は、この復号した使用可能回数Ｎを状態表示メモリ４０７に書き込み、比較手段４０９に通知していくとともに、この復号した鍵ＫＵを第３の復号手段４０６に通知していく。

【００４３】第２の復号手段４０５から使用可能回数Ｎの通知を受け取ると、比較手段４０９は、通知を受けた使用可能回数Ｎがゼロ値であるか否かをチェックして、ゼロ値であるときには状態表示メモリ４０７をクリア処理し、ゼロ値でないときにはこのクリア処理を実行しないよう処理する。一方、第３の復号手段４０６は、第２の復号手段４０５から鍵ＫＵの通知を受け取ると、ソフトウェア記憶媒体１のＲＯＭ領域に書き込まれている暗号ソフトウェア“E_{KU}（ＤＡＴＡ）”を、この通知を受けた鍵ＫＵでもって復号することで、提供対象となるソフトウェアを生成し、出力手段４１１は、この復号されたソフトウェアを図示しない出力機器に出力していく。このとき、第３の復号手段４０６は、状態表示メモリ４０７がクリアされているときには、この復号処理を実行できない。

【００４４】すなわち、ソフトウェア記憶媒体１に記録される使用可能回数Ｎがゼロ値であるときには、ソフトウェア読取装置４は、ソフトウェア記憶媒体１に記録されたソフトウェアの使用を実行できないように動作していくのである。

【００４５】この処理にあって、カウンタ４０８は、状態表示メモリ４０７に展開された使用可能回数Ｎを計数値の初期値として読み込んで、第３の復号手段４０６がソフトウェアの復号を行うと、この復号処理に同期させて計数値をカウントダウンする。このとき、比較手段４０９は、このカウンタ４０８の計数処理を受けて、計数値Ｎ’がゼロ値に達したか否かをチェックして、ゼロ値に達するときには、ソフトウェアの使用を禁止するために状態表示メモリ４０７をクリアしていく。

【００４６】そして、“ＥＯＦ”に従ってソフトウェアの使用の終了が検出されると、第２の暗号化手段４０１は、カウンタの計数値Ｎ’と鍵ＫＵとを、鍵ＫＹでもって暗号化することで、使用可能回数の減じられた新たな暗号ソフトウェア保護情報“E_{KY}（KU，N）”を生成

する。続いて、第３の暗号化手段４０２は、この第１の暗号化手段４０１の出力する暗号ソフトウェア保護情報“E_{KY}（KU，N）”を、鍵KXでもって暗号化することで、使用可能回数の減じられた新たな暗号ソフトウェア保護情報“E_{KX}（E_{KY}（KU，N））”を生成して、ソフトウェア記憶媒体１のＲＡＭ領域の暗号ソフトウェア保護情報をこの新たなものに書き換えていく。

【００４７】一方、“ＥＯＦ”に従ってソフトウェアの使用の終了が検出されると、書込手段４１０は、カウンタの計数値N’を新たな使用可能回数として、この使用可能回数を制御情報の一部としてソフトウェア記憶媒体１のＲＡＭ領域に書き込んでいくとともに、第４の暗号化手段４０３は、状態表示メモリ４０７から読み出す装置パラメータ状態情報を規定の変換鍵でもって暗号化してから、制御情報の一部としてソフトウェア記憶媒体１のＲＡＭ領域にメンテナンス等のために書き込んでいく。

【００４８】このようにして、ソフトウェア読取装置４は、ソフトウェア記憶媒体１に記録される暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能回数を得ると、この使用可能回数がゼロ値を表示していないときには、暗号ソフトウェア保護情報の復号により得られる鍵情報を用いて暗号ソフトウェアを復号してユーザに提供していくとともに、使用終了毎に使用可能回数を減算してソフトウェア記憶媒体１の暗号ソフトウェア保護情報を更新し、一方、この使用可能回数がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理するのである。

【００４９】この構成に従い、本発明では、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになって、不正使用の防止を図れることになる。

【００５０】この使用形態を採るソフトウェア記憶媒体１のソフトウェアの使用状態を管理する管理装置５は、図６に示すように、記憶媒体読取手段５００と、モデム手段５０１と、復号手段５０２と、照合分別手段５０３と、集計比較手段５０４と、登録媒体ファイル５０５と、販売店ファイル５０６と、ユーザ情報・ソフトカタログファイル５０７と、出力手段５０８とを備える。

【００５１】この装置構成を採るときにあって、復号手段５０２は、バージョンアップしたソフトウェアの書込要求等に従って通信路や販売店を介してソフトウェア記憶媒体１が回収されると、そのソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報を規定の変換鍵でもって復号することで、そのソフトウェア記憶媒体１に記録されている使用可能回数を読み取って、照合分別手段５０３を介して集計比較手段５０４に通知する。

【００５２】一方、照合分別手段５０３は、記憶媒体読取手段５００やモデム手段５０１から、回収されたソフトウェア記憶媒体１の識別番号を受け取ると、登録媒体ファイル５０５を参照することで、そのソフトウェア記憶媒体１の製造情報を収集し、販売店ファイル５０６を参照することで、そのソフトウェア記憶媒体１の販売店を特定し、ユーザ情報・ソフトカタログファイル５０７を参照することで、そのソフトウェア記憶媒体１を使用したユーザ情報や、そのソフトウェア記憶媒体１に記録されているソフトウェア情報を収集して、その収集・特定結果を集計比較手段５０４に通知する。

【００５３】この収集・特定結果を受け取ると、集計比較手段５０４は、照合分別手段５０３から通知される製造情報に従って、ソフトウェア記憶媒体１に記録された製造時点での使用可能回数をソフトウェア記憶媒体１の識別番号を単位に特定する。そして、復号手段５０２から通知される使用可能回数をソフトウェア記憶媒体１の識別番号を単位に集計し、製造時点での使用可能回数とこの集計値との差分値とからソフトウェアの使用回数を特定して、この特定した使用回数が製造時点での使用可能回数を上回っているか否かをチェックして、そのチェック結果を出力手段５０８に出力する。

【００５４】この構成に従い、本発明では、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。そして、この構成にあって、ソフトウェア記憶媒体１の販売先ユーザ名が特定できるようになっていると、どのユーザが不正複写等の不正使用をしたのかも特定可能となるのである。

【００５５】図示実施例について説明したが、本発明はこれに限定されるものではない。例えば、実施例では、ソフトウェアの使用可能回数の初期値を出荷元で記録していく構成を開示したが、本発明はこれに限られることなく、流通途中の販売店で記録するようにしてもよいのである。また、実施例では、製造時点での使用可能回数がゼロ値に達すると、ユーザサイドでは、使用可能回数の追加を一切認めない構成を開示したが、本発明はこれに限られることなく、使用可能回数の追加を認めていくようにしてもよいのである。また、実施例では、ソフトウェア記憶媒体１を販売する利用形態のもので開示したが、本発明はこれに限られることなく、貸し出す形態のものであってもよいのである。

【００５６】

【発明の効果】以上説明したように、本発明によれば、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソ

13

フトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになる。しかも、流通途中で暗号構造を変更していくことで、出荷元と中継先との間での不正使用は完全に排除できることになる。

【００５７】そして、本発明によれば、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。しかも、ソフトウェアの流通先を記録しておくことが可能であるならば、誰が不正複写等の不正使用をしたのかも特定可能となる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の適用される流通システムの一例である。

【図３】出荷元装置の装置構成の一実施例である。

【図４】中継先装置の装置構成の一実施例である。

【図５】ソフトウェア読取装置の装置構成の一実施例である。

14

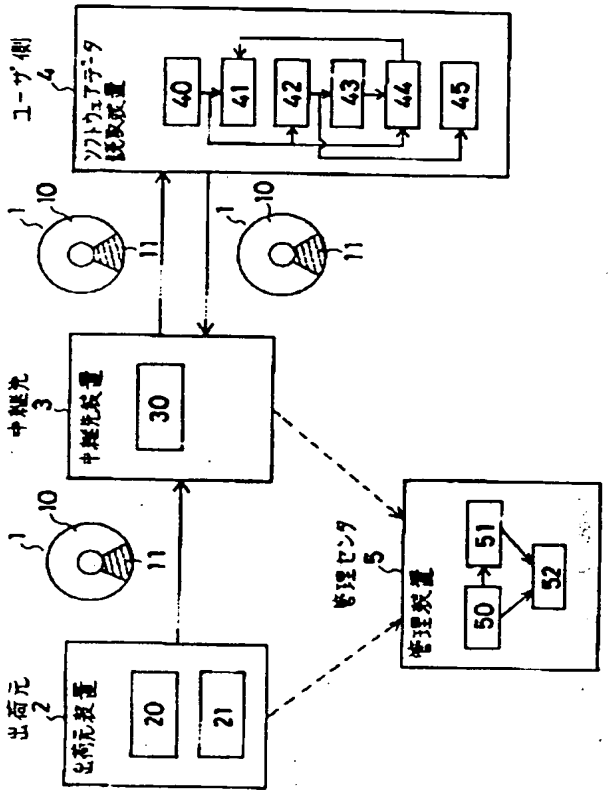
【図６】管理装置の装置構成の一実施例である。

【符号の説明】

1　ソフトウェア記憶媒体
2　出荷元装置
3　中継先装置
4　ソフトウェア読取装置
5　管理装置
１０　書換不可能記憶領域
１１　書換可能記憶領域
２０　第１の書込手段
２１　第２の書込手段
３０　暗号構造変更手段
４０　第１の復号手段
４１　第２の復号手段
４２　算出手段
４３　更新手段
４４　抑止手段
４５　設定手段
５０　第１の集計手段
５１　第２の集計手段
５２　比較手段

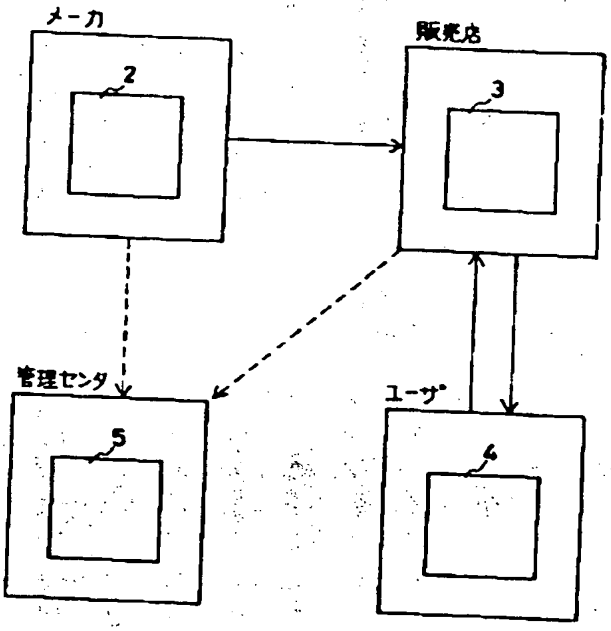
【図１】

本発明の原理構成図



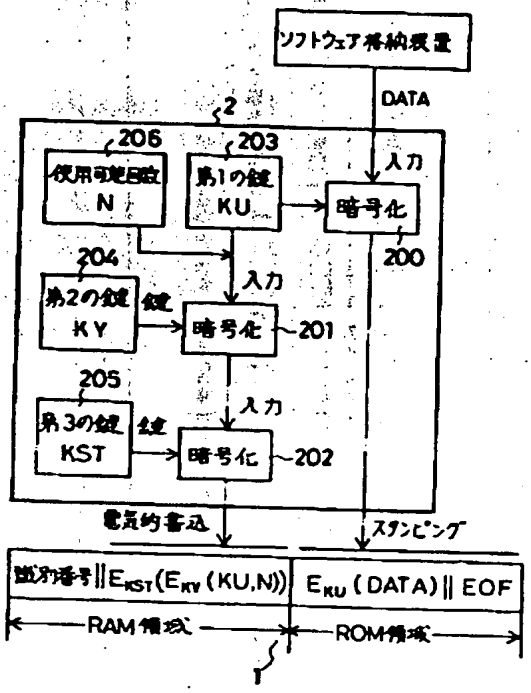
【図２】

本発明の適用される流通システムの一例



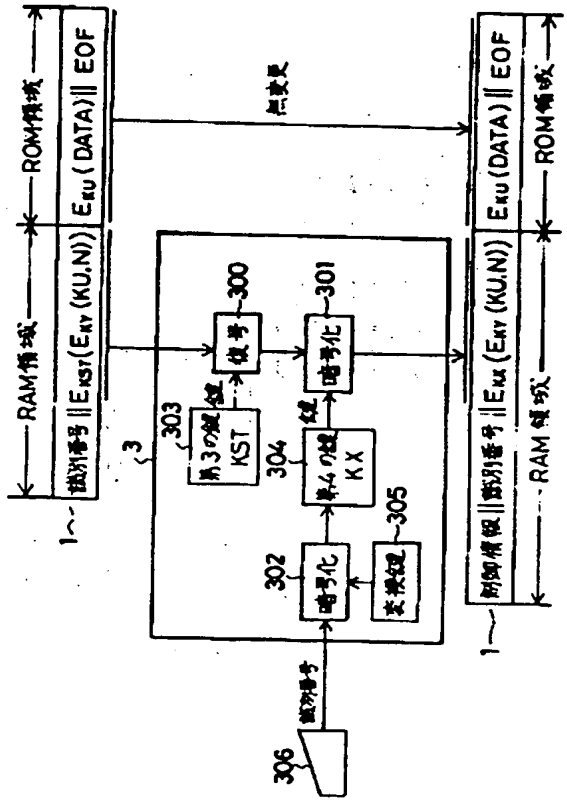
【図3】

出荷元装置の装置構成の一実施例



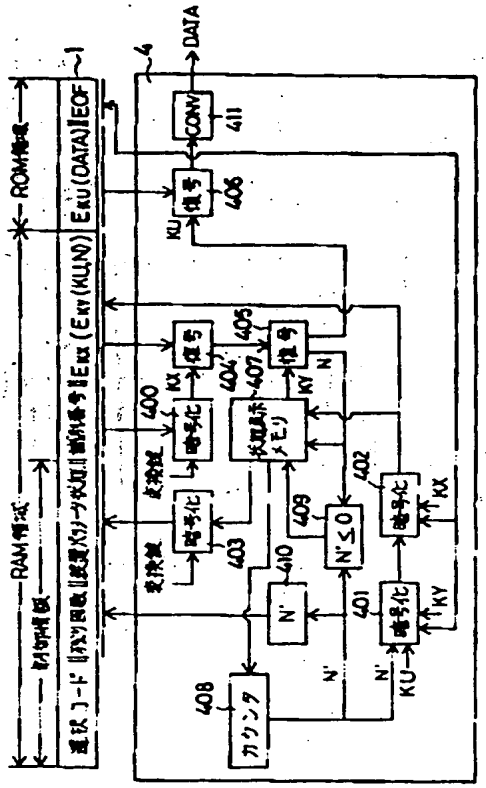
【図4】

中継先装置の装置構成の一実施例



【図5】

ソフトウェア読取装置の装置構成の一実施例



【図6】

管理装置の装置構成の一実施例